MODERN ATTACKS AGAINST RUSSIAN FINANCIAL INSTITUTIONS

Jean-Ian Boutin & Anton Cherepanov
ESET, Slovakia

Email {boutin, cherepanov}@eset.sk

ABSTRACT

Attacks on Internet banking users are no longer breaking news. In fact, several different banking trojans have, for almost a decade, been targeting Internet users making online banking transactions. These attacks are now routine even though the different attackers are constantly changing their methods and tools, as well as adjusting their techniques to counter the security measures introduced by defenders. However, something new has developed in the past few years: the rise of organized, specialized cybercriminal groups directly targeting financial institutions instead of their customers.

This trend has been seen in several countries, but banks in Russia seem to be targeted most frequently. It is now common to see an attacker group trying to spear-phish workers in these banks with the ultimate goal of stealing money by making fraudulent transfers or using other elaborate schemes. Some of them are also showing particular interest in the trading platforms used by the banks. We have seen a case where cybercriminals successfully gained unlawful access to a trading platform where they could issue orders on behalf of a victim bank. There have been some regulatory changes introduced in Russia lately, but this has not stopped the cybercriminals. We have even seen groups impersonating this new government body in order to better to lure their targets.

This paper will cover different groups targeting financial institutions worldwide, but especially in Russia. We will look at long lasting gangs, such as Buhtrap and Corkow, that have been relentlessly targeting the Russian financial sector. These groups are highly sophisticated and are spending a large amount of time compromising different entities to improve the coordination of their attacks. They also infiltrate the corporate network for a long time, finding the right workstation and carefully planning their final attack. Some groups use a shotgun approach where they try to infect as many computers as possible and then run tools to find the interesting ones, while others are doing background research before conducting their attacks and attempt to compromise only interesting targets. This paper will review the different tactics and tools used by the different groups. Another interesting aspect of these attacks is the usage of code-signing certificates. In fact, one group has used more than 20 different code-signing certificates in the past two years. A description of how these tools were used, the different attacks they performed and an estimate of the amounts that were stolen will also be given.

Finally, we will try to determine whether these types of attacks are likely to transfer to the rest of the world, as is often the case with Russian cybercrime. In fact, we have seen countless examples of Russians being the first victims of trends that are subsequently globalized.

INTRODUCTION

Cybercriminals around the world have targeted online banking users for almost a decade now. While there is still money to be made from this activity, we are seeing more and more creative cybercriminals directly targeting banks instead of individuals or businesses. By doing so, they are able to steal millions of dollars from these entities.

There are more than 600 banks in Russia and not all of them have the same security measures. In the past few years, a growing number of organized and specialized groups have been robbing these financial institutions with the aid of malware. In this paper, we will try to shed some light on some of these groups and their tactics.

What makes these types of attacks so interesting is the fact that the groups perpetrating them are highly specialized. While studying their tactics, we can make several connections to traditional so-called APT groups targeting different organizations for espionage. While the motive is different – financial gain in the case of these actors – the fact that they research their targets before attacking them, the way the hosts are compromised through spear phishing or strategic web compromise, and the fact that they are likely to persist in a network and study their victims for a lengthy period of time, is characteristic of more traditional espionage groups. Once they have a foothold in a targeted organization, they will try to reach interesting systems through lateral movement and learn more about the organization and its structure to ensure a smooth process when the time for their evil deeds comes.

They also use several techniques to blend in and hide the fact that a major breach has occurred. They commonly use third-party utilities, like a remote administration tool, to control a workstation. Some groups also use big, common botnets and cherry-pick the victims onto whose PCs they drop more sophisticated tools. Some groups build their own botnets while others buy compromised workstations from a fellow cybercriminal. Their use of off-the-shelf penetration test tools also makes attribution harder. As these attacks are usually kept secret by the targeted financial institutions, it is also hard to build a clear picture of the threat.

With concerns growing over attacks on their banks, in May 2015 the Russian government created a new CERT, FinCERT [1], whose responsibility is to tackle cybercrime targeting Russian financial institutions. Their mandate includes:

- Sharing information about attacks
- Providing analysis of tactics and tools used by cybercriminals
- Providing recommendations for best practice in information security for financial institutions.

Despite this new organization, financial crime against Russian financial institutions is still increasing. Moreover, the Russian Central Bank suspects that some banks are actually using cyber attacks as a way to hide previous attacks or to withdraw funds.

Mr Georgy Luntovskiy, First Deputy Governor of the Bank of Russia, stated that three of the banks that had previously been subjected to cyber attacks had lost their licences [2]. In fact, cybercriminal groups can impair the financial stability of the targeted institutions by successfully stealing large amounts of money from them.

Interestingly, in the past few months, there have been a growing number of cases of banks being targeted in different regions of the world. What has started mainly as a Russia-centric phenomenon has clearly grown to the point where all financial institutions worldwide should take measures to prevent the types of fraud we will outline in the following sections.

In the first part of this paper, we will survey some of the groups perpetrating attacks on Russian financial institutions. We will then review the tools, tactics and procedures (TTPs) these groups use. The following section will discuss the different systems that are targeted by cybercriminals for financial gain.

Finally, we will try to determine whether these types of attacks are likely to migrate to the rest of the world, as is often the case with Russian cybercrime. In fact, we have seen countless examples of Russians being the first victims of trends that are subsequently globalized.

GROUPS PERPETRATING THESE ATTACKS

There are not that many groups with the capabilities needed to perform large financial thefts like the ones this paper considers. The following are some groups who possess the necessary organization and sophistication to be able to pull off this type of cyber heist:

Corkow

- **Alternative name:** Metel
- **First appearance:** 2011
- **Targets:** banks; various businesses
- **Infection vectors:** exploit kits; spear phishing

The Corkow group [3] has existed at least since 2011. This group uses custom modular malware detected by *ESET* as Win32/Corkow.

The group behind Corkow successfully compromised a trading terminal in a Russian bank, allowing them to trade on Moscow Exchange, the largest exchange group in Russia, through the financial institution's trading account. In February 2015, the attackers made several currency sale and purchase operations using the compromised trading terminal on behalf of the bank. As a result of this activity, the bank claimed losses of 244 million rubles (US$3.2 million) [4].

Another notorious case involving the Corkow group was noted in August 2015. The group successfully hacked a card processing centre, which allowed fraudsters to withdraw an estimated 500 million rubles (US$7.7 million) from ATMs [5].

According to *ESET LiveGrid* telemetry, the majority of detections are seen in Russia and Ukraine. At its peak, Corkow's botnet size was estimated at 300,000 infected computers.

The main infection vector used by this group is the Niteris Exploit Kit, a kit available only to trusted users. In order to find valuable targets, this group mainly uses a 'shotgun' approach. They try to grow their botnet as much as possible and subsequently find interesting and valuable infections. The Corkow group also uses spear-phishing emails with Rich Text Format (RTF) documents embedding exploits for *Microsoft Word*.

This group is highly specialized and has attacked financial institutions with proper security measures. The fact that they were able to devise an attack on trading terminals clearly showcases their technical expertise. It also highlights a fact that is becoming more and more common in these attacks: the malware used is no longer central to the heist. It is just a tool used by resourceful criminals to attain their goal.

Carbanak

- **Alternative name:** Anunak
- **First appearance:** 2013
- **Targets:** banks; media/PR companies; retail; various businesses
- **Infection vectors:** spear phishing; selected victims in wider botnet; exploit kits

Starting in 2013, the Anunak [6] / Carbanak [7] group successfully stole millions from several banks, primarily in Russia. The group is very organized, capable of mounting and executing complex heists targeting financial institutions with strong defences. Although they were successful in robbing many banks in Russia, they also expanded their activities to target businesses elsewhere.

This group commits financial fraud in many different ways, but probably the most spectacular was their ability to control ATMs remotely to dispense cash at pre-defined times [8]. Accomplices would wait around the ATM until it started to automatically dispense cash, put the money in bags, and leave the scene without ever touching the ATM.

The main infection vector used by this group is spear phishing, but they also use exploit kits and select valuable victims from existing botnets. Once they have a foothold in a financial institution, they attempt to perform lateral movement to extend their network within the compromised company. They also deploy tools allowing them to spy on their victims and study their behaviour for weeks or even months before attempting any heist.

Buhtrap

- **Alternative name:** Ratopak
- **First appearance:** 2014
- **Targets:** banks; various businesses
- **Infection vectors:** spear phishing; exploit kits; strategic web compromise (a.k.a. watering hole attack)

This group appeared on our radar in 2014 and has been targeting Russian and Ukrainian businesses and financial institutions relentlessly [9]. Their main infection technique is spear phishing, although they have also been using exploit kits and strategic web compromise in some campaigns. Once they have a foothold in the targeted institution, they use a variety of custom and third-party tools to learn more about the network and behaviour of their victims.

ESET telemetry shows that the majority of detections for this group's malware occurred in Russia. Although they first targeted various types of Russian businesses, they soon turned their attention to financial institutions and, as such, might be the best illustration of groups transitioning from online banking users to the banks themselves. Although they were targeting specific individuals within financial institutions, they were targeting so many of them that discovering an attempted targeted attack on a Russian bank was no longer unusual. From August 2015 to February 2016, Buhtrap conducted 13 successful attacks on Russian banks for a total amount of 1.8 billion rubles (US$25.7 million) [10].

In fact, this group is unique in the way it spreads its tools, as they are dropped at the very beginning of the breach. The other groups tend to carefully choose the workstation on which they will deploy their most interesting tools, making the Buhtrap group 'louder' than the others.

In February 2016, the source code for most of their tools was leaked in underground forums. This was following several successful heists they had committed against several Russian banks. The message advertising the leak, posted on underground forum *exploit.in*, was from a disgruntled coder, complaining that he was not paid enough. The veracity of this statement could not be confirmed.

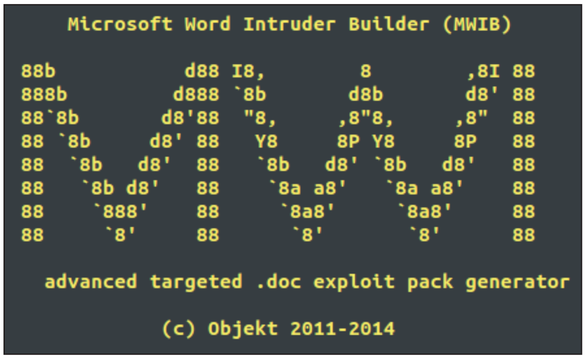
Similarities

While there are other groups targeting banks, these are the major ones according to our tracking data. Common to all these groups is their professionalism and organizational capability. They are well-organized, APT-style groups with clear goals and member specialization. They research their targets beforehand for maximum efficiency and have deep knowledge of how bank systems and custom tools work.

These groups are composed of different people, each with different roles [11]. Some are regular employees while others are contractors who work for a fixed amount of money to produce software or perform specific tasks. The group usually comprises regionally distributed individuals and the leaders have strong ties with different actors in the Russian-speaking underground.

As stated above, these groups usually rely on contractors or third parties offering a variety of tools. Through them it is possible to draw weak links between these groups. For example, both the Buhtrap and Corkow groups used Niteris EK [12] as an infection vector. This kit is available only to trusted users, so the Corkow and Buhtrap groups share a common connection. Moreover, in various watering hole attacks, accounting portals or specialized websites for the registration of legal entities were redirecting to Niteris EK, and distributing either Buhtrap or Corkow malware to unsuspecting visitors [10].

They also all share a common infection vector: spear phishing with malicious attachments. In fact, all of them used either the same old exploits against *Microsoft Office*, or macros, to try to gain entry to the institutions' systems. Some of them have used third-party tools such as the Microsoft Word Intruder (MWI) kit [13], a framework sold to selected customers to automatically create RTF documents exploiting several known *Word* vulnerabilities.



```
    Microsoft Word Intruder Builder (MWIB)

88b           d88 I8,        8        ,8I 88
888b         d888 `8b       d8b       d8' 88
88`8b       d8'88  "8,     ,8"8,     ,8"  88
88 `8b     d8' 88   Y8     8P Y8     8P   88
88  `8b   d8'  88   `8b   d8' `8b   d8'   88
88   `8b d8'   88    `8a a8'   `8a a8'    88
88    `888'    88     `8a8'     `8a8'     88
88     `8'     88      `8'       `8'      88

  advanced targeted .doc exploit pack generator

            (c) Objekt 2011-2014
```

Figure 1: MWI logo as seen in kit documentation.

This is a common pattern and a lot of attacks perpetrated by these groups were preventable by applying basic countermeasures. Attackers will concentrate on the weakest link. As security measures to protect online banking users increase in efficiency, cybercriminals will turn towards easier and more lucrative targets, as some institutions' security processes are inadequate.

Once they get inside an organization, these groups will study their targets and install third-party tools for lateral movement or remote control. They all use *Ammyy*, *LiteManager* or a similar tool to control workstations remotely. The use of these tools makes breach detection harder as they are commonly used within these organizations. They also modify system settings to allow multiple remote sessions on a single computer. Some of them will also try to make malware analysis harder by encrypting key components of their toolset with a user-specific key. Corkow and Buhtrap encrypt their main DLLs using the hard drive serial number as a key. Execution on a different machine is thus impossible. This technique is not widely used in targeted attacks, making this additional connection between the groups interesting. The technique has been used in the past by malware such as Flashback and Rustock, but it is not widespread.

Once the campaign is completed, these groups cover their tracks. Carbanak and Buhtrap both overwrite the machine's master boot record (MBR) to make it unbootable. Corkow also has an 'uninstallation' command with a parameter used to destroy the machine's MBR.

While there are similarities between the ways these groups operate, we believe that they are different entities, as the main malware they use is quite different.

Apparent from the similarities between these groups, we can also infer that they influence each other. In fact, since the Carberp group arrest [14] and the subsequent code leak, its influence can be seen in many places in the Russian cybercrime landscape. Many believe that past members of the Carberp gang are now in the Carbanak group, and that in fact the main payload was based on Carberp code (hence the group name). Looking at the threat landscape, the Carberp group has had a lasting effect on cybercrime in Russia.

TACTICS, TOOLS AND PROCEDURES

In this section, we will examine the different tactics, tools and procedures used by these advanced groups at each stage of the attack.

Point of entry

While the final goal of the attack is the same, the groups are using different techniques to gain an initial foothold in the different financial institutions. The preferred methods are usually via emails or through drive-by downloads, especially strategic web compromise (SWC), a technique popularized by APT actors.

Shotgun vs. targeted approach

Groups like Buhtrap and Carbanak usually prefer using targeted attacks where they will send spear-phishing emails to selected individuals working in financial institutions of interest. They may use either malicious links or malicious attachments to infect their targets. Both groups employed Microsoft Word Intruder kit, a kit advertised in underground forums [15]. This kit contains exploits for several different CVEs targeting *Microsoft Word* and can thus adapt to different *Microsoft Office* versions that might be installed on different targets.

The Buhtrap group uses something of a hybrid technique, somewhere between the shotgun and targeted approaches. We classify it as 'targeted' since they mostly use spear phishing, but they use a lengthy list of recipients. They send waves of spear-phishing attacks, using different subjects such as an invitation to a conference or fake job offers [16].

Another technique we have seen these groups use is to try to compromise websites that are likely to be visited by their targets. In one case, Buhtrap installers were bundled with the legitimate *Ammyy Admin* installer and distributed through the official *Ammyy* website [17]. Since this group is extensively using remote administration tools in its activities, compromising this website is a logical choice. We are unsure, however, whether they used it in conjunction with social engineering, cold-calling their targets and asking them to go to the legitimate website to download *Ammyy Admin*, or if they were only trying to compromise a large number of *Ammyy Admin* users.

Some groups are also leveraging existing botnets or implementing their own to reach their targets. They have good ties with big botnet operators from which they can buy access to selected financial institutions. Others, like Corkow, prefer to compromise as many workstations as possible and will then search for hidden gems via their admin panel. Although this technique does not allow the cybercriminals to pick their targets, the fact that the Corkow group uses Niteris EK still makes these attacks more targeted than regular crimeware. In fact, Russian accounting portals were redirecting their visitors to Niteris EK, meaning that they were, to a certain degree, able to control who would receive their payload.

Figure 3 shows the classic infection steps that these groups use.

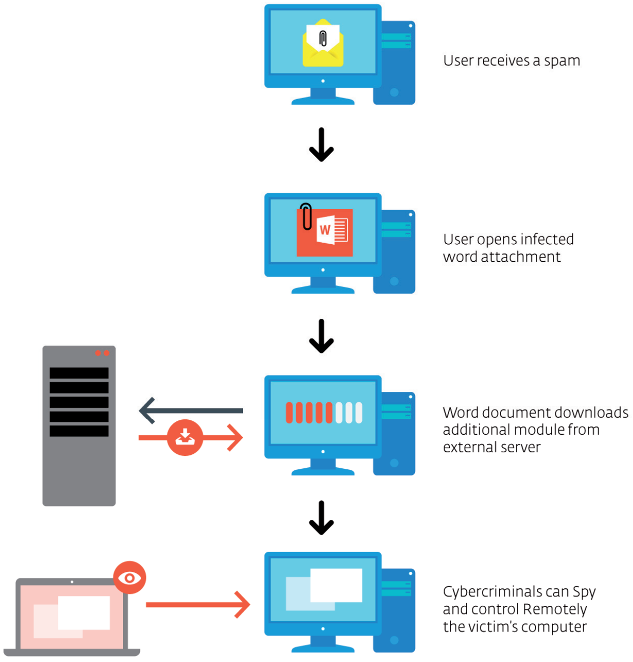
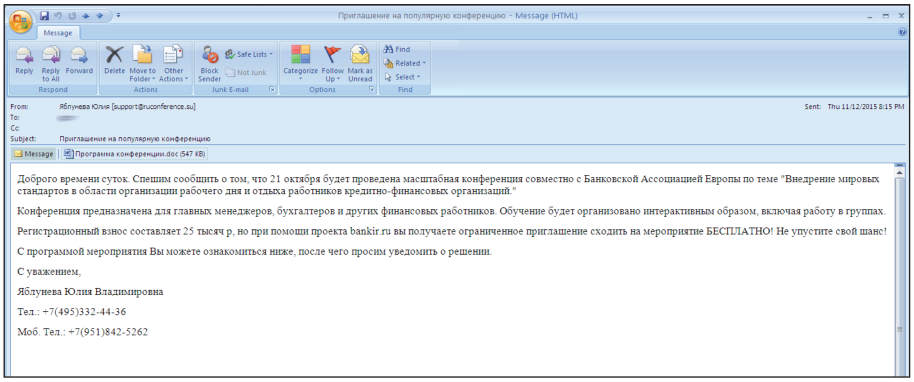

User receives a spam
User opens infected word attachment
Word document downloads additional module from external server
Cybercriminals can Spy and control Remotely the victim's computer

Figure 3: Common infection pattern.



From: Яблунева Юлия [support@ruconference.su]
To: [redacted]
Cc:
Subject: Приглашение на популярную конференцию
Sent: Thu 11/12/2015 8:15 PM

Message | Программа конференции.doc (547 KB)

Доброго времени суток. Спешим сообщить о том, что 21 октября будет проведена масштабная конференция совместно с Банковской Ассоциацией Европы по теме "Внедрение мировых стандартов в области организации рабочего дня и отдыха работников кредитно-финансовых организаций."

Конференция предназначена для главных менеджеров, бухгалтеров и других финансовых работников. Обучение будет организовано интерактивным образом, включая работу в группах.

Регистрационный взнос составляет 25 тысяч р, но при помощи проекта bankir.ru вы получаете ограниченное приглашение сходить на мероприятие БЕСПЛАТНО! Не упустите свой шанс!

С программой мероприятия Вы можете ознакомиться ниже, после чего просим уведомить о решении.

С уважением,

Яблунева Юлия Владимировна

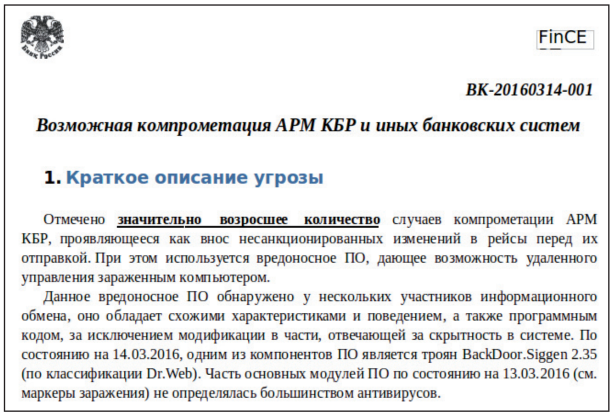
Тел.: +7(495)332-44-36

Моб. Тел.: +7(951)842-5262

Figure 2: Spear-phishing email sent to a bank employee, inviting him to a conference.

Impersonating legal entities

In order to increase the probability of their victim opening the attachment or clicking on the link, many of these groups try to impersonate legitimate entities. In the introduction, we discussed how the Russian government created a new organization to provide help and guidance to Russian financial institutions defending against cybercrime. It did not take long before this organization was impersonated in a decoy document, as shown in Figure 4.



Банк России

FinCE

BK-20160314-001

Возможная компрометация АРМ КБР и иных банковских систем

1. Краткое описание угрозы

Отмечено **значительно возросшее количество** случаев компрометации АРМ КБР, проявляющееся как внос несанкционированных изменений в рейсы перед их отправкой. При этом используется вредоносное ПО, дающее возможность удаленного управления зараженным компьютером.

Данное вредоносное ПО обнаружено у нескольких участников информационного обмена, оно обладает схожими характеристиками и поведением, а также программным кодом, за исключением модификации в части, отвечающей за скрытность в системе. По состоянию на 14.03.2016, одним из компонентов ПО является троян BackDoor.Siggen 2.35 (по классификации Dr.Web). Часть основных модулей ПО по состоянию на 13.03.2016 (см. маркеры заражения) не определялась большинством антивирусов.

Figure 4: Decoy document showing a bogus FinCERT advisory.

In this particular attack, run by the Buhtrap group, they also registered many domains with the FinCERT theme, again trying to legitimize their spear-phishing email. As is often the case with APT groups, significant care is taken by these groups when choosing domains that are used as C&Cs.

Group-IB reported [10] that, in one particularly bold move, Buhtrap sent a phishing attack to a trusted mailing list impersonating Gazprombank, the third-largest bank in Russia. As these lists are not accessible to the general public and emails usually come from trusted members, this adds a layer of legitimacy. In this case, the fraud was discovered quickly.

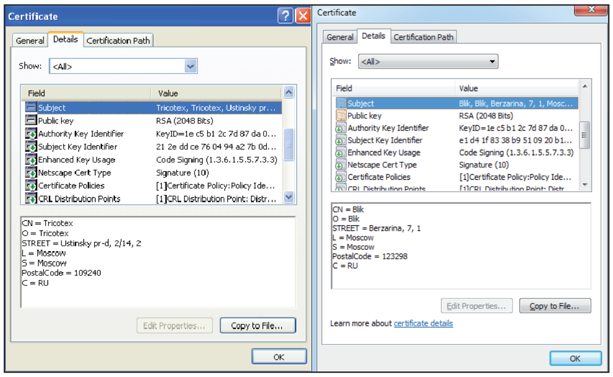
Code-signing certificates

Carbanak and Buhtrap have both used several code-signing certificates. Several examples of their malware were signed by these certificates to increase their apparent legitimacy. Buhtrap used more than 20 certificates, all sharing a common feature, even amongst the ones that were used by Carbanak group: they were all awarded to Russian companies (e.g. wholesalers and builders) that do not immediately look like they develop code that needs to be signed. Also, we found in our databases only malicious files that were signed by these certificates, no legitimate files.

The Buhtrap group seemed able to get an endless supply of code-signing certificates. The first time we would see them appear in the wild was often a couple of months after they had been awarded.

Reconnaissance

Once an organization has been breached, some checks are run on the machine, either manually or automatically, to assess its value. Corkow's operator will check basic information that was initially collected on a compromised system through the administration panel and will then decide to drop a remote administration tool, usually *Ammyy* or the Visconti Backdoor, if further investigation is necessary. Once a manual check has been done, they can decide whether additional tools should be used. Carbanak was also doing similar checks before downloading and executing its main component on any given system.



Field	Value
Subject	Tricotex, Tricotex, Ustinsky pr...
Public key	RSA (2048 Bits)
Authority Key Identifier	KeyID=1e c5 b1 2c 7d 87 da 0...
Subject Key Identifier	21 2e dd ce 76 04 94 a2 7b 0d...
Enhanced Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Netscape Cert Type	Signature (10)
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr...

```
CN = Tricotex
O = Tricotex
STREET = Ustinsky pr-d, 2/14, 2
L = Moscow
S = Moscow
PostalCode = 109240
C = RU
```

Field	Value
Subject	Blik, Blik, Berzarina, 7, 1, Mosc...
Public key	RSA (2048 Bits)
Authority Key Identifier	KeyID=1e c5 b1 2c 7d 87 da 0...
Subject Key Identifier	e1 d4 1f 83 38 b9 51 09 20 b1...
Enhanced Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Netscape Cert Type	Signature (10)
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr

```
CN = Blik
O = Blik
STREET = Berzarina, 7, 1
L = Moscow
S = Moscow
PostalCode = 123298
C = RU
```

Figure 5: Code-signing certificates used by Buhtrap (left) and Carbanak (right) display similarities.

Buhtrap does something similar, but has automated all these checks and will download additional packages only if the system successfully passes all the checks. They first check for signs of a sandbox or a malware analyst's computer, then make sure that the workstation is using either the Russian or Ukrainian language, and finally will check the list of processes and typed URLs for signs of banking applications. If these tests are successful, an additional package containing tools to monitor the workstation, a backdoor and pentesting tools, is dropped and executed on the machine.

Trying to avoid unnecessary installation of custom tools is understandable. Since these attacks are targeted, samples are not easy to find for security companies and thus usually go undetected for a long time. It also makes it harder for malware researchers to get hold of these samples and actively track the group before an attack is successful. The extent of a group's tools is often known only when an external company is called in to perform an incident response.

Lateral movement

These groups are usually trying to expand their network of compromised systems in an institution of interest. They wish to find *the* workstation that will bring them maximum revenue, but also to persist as long as possible in the organization's network should one workstation be cleaned or decommissioned.

Common penetration testing tools such as Metasploit and MimiKatz – tools that can retrieve *Windows* account passwords from memory – are frequently used. They will also scan for RDP/VNC and network ports to reach interesting workstations. Buhtrap had automated tools that could create additional accounts on a given workstation once administration rights were obtained.

To be able to run these tools, sometimes local privilege escalation (LPE) exploits are needed. This is one case where contacts with other underground actors become invaluable. Groups like these will be able to buy and have at their disposal several different LPEs that they can use depending on which *Windows* version they are executing.

The Holy Grail in these situations is often the domain controller where they can obtain credentials for all active domain accounts. Once the right workstations are compromised, the cybercriminals will lurk on the network, gathering as much information as possible to make their attack successful.

Study of victim behaviour

Monitoring tools are deployed on key workstations. Corkow and Carbanak both have modules able to take screenshots and videos and upload them to the C&C server. Using these images and videos, the cybercriminals can learn more about how their victims are operating, a vital procedure if one wants to connect back to their workstations and perform tasks without raising red flags.

The main components of Corkow and Buhtrap are also able to detect when a smart card is present in a system. In order to issue financial orders, usually the system requests the employee to have his smart card inserted and unlocked. The malware can detect when the smart card is present in an attempt to bypass this additional security measure. Corkow also has an interesting additional feature: it is able to tell whether someone is currently using the computer by monitoring the mouse and keyboard inputs. This allows the operators to learn the workstation user’s break and lunch habits.

To extend their knowledge of the institution’s structure and capabilities, some groups actively try to access mail servers to monitor emails from employees. They can then specifically target the emails coming from the information security department. That way, they can learn when an anomaly is discovered and how the anomaly is resolved. This is a great source of information while trying to assess how best to conduct their heist.

Theft

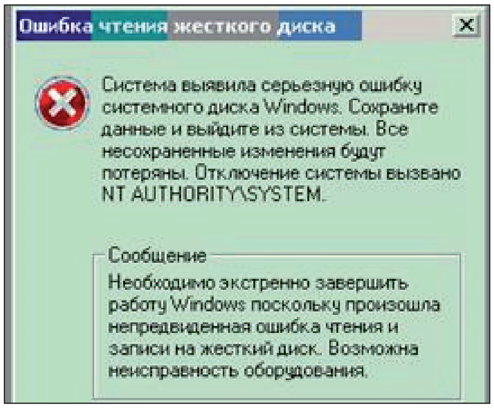
All of these groups are (ab)using remote administrator tools, most of them third-party tools like *Ammyy Admin*, *LiteManager* or *TeamViewer*. The final intent is to be able to mimic the worker’s behaviour while performing transfers or other malicious activities through the remote administrator tool. In fact, in some cases they do not even need to deploy their main malware on all the machines, as having a remote administration program installed is enough.

However, sometimes the remote administrator tool is not enough, as custom applications are used by their targets. To get around this, the attackers need to develop their own custom tools.

There are many ways to steal money from financial institutions, and each way requires a custom methodology. Whether the cybercriminals want to wire funds through SWIFT, make ATMs dispense money automatically, play with internal databases to modify account balances, or issue financial orders, they need to know the different systems inside and out. They can gather this information by spying on their victims or, more conveniently, have someone in their group with this knowledge. Either way, this shows that these people have become experts at what they do.

Covering their tracks

After they are done with a specific computer, these groups try to hide their tracks. Corkow malware can receive a SelfRemove command with the parameter DestroySystem that will not only overwrite the MBRs of all physical drives, but will also delete registry keys and overwrite configuration files with random data. Carbanak and Buhtrap use a similar tool that will erase the MBR, effectively making the computer unbootable. The Buhtrap gang also shows a message to the user saying that there has been a hard drive failure, adding credibility to the fact that the computer is no longer bootable. The likely result of this action is that their IT department will re-image the machine, making forensic work after the attack much harder.



Ошибка чтения жесткого диска

Система выявила серьезную ошибку системного диска Windows. Сохраните данные и выйдите из системы. Все несохраненные изменения будут потеряны. Отключение системы вызвано NT AUTHORITY\SYSTEM.

Сообщение

Необходимо экстренно завершить работу Windows поскольку произошла непредвиденная ошибка чтения и записи на жесткий диск. Возможна неисправность оборудования.

Figure 6: Message shown to user after Buhtrap MBR eraser malware was run, claiming that there was a problem with the hard drive and that a reboot is necessary.

As discussed previously, another trick that is used by Buhtrap and Corkow to hinder forensics is the use of a system-dependent encryption key to encrypt key components on the victim’s computer.

TARGETED SYSTEM

When attackers get inside a financial institution’s internal network, they can abuse different systems to achieve financial gains.

Attacks on ATMs and bank card systems

This is by far the most spectacular category of attack and was used by both Corkow and Carbanak groups. Depending on the ATM model, the *modus operandi* is different. The first group was able to perform a rollback attack using the bank card system where they would withdraw money from an ATM and then do a ‘rollback’ on the account balance so that they could repeat the withdrawal process over and over again [18].

Carbanak was able to connect to ATMs through compromised workstations within the bank network. One strategy they used was to change the banknote denominations dispenser so that an accomplice could ask to withdraw, for example, ten 100 ruble banknotes and would instead receive ten 5,000 ruble banknotes [6]. In another case, they remotely controlled the ATM, instructing it to give out money at specific times, without the need for anyone to interact with it physically [7].

Such attacks on ATMs can result in huge financial losses for the affected banks, often running to millions of dollars.

Attacks on SWIFT terminals

Another way for cybercriminals to make money while lurking in the financial institution's network is to find and compromise workstations used to make SWIFT transfers. SWIFT is an international transfer system used by banks all around the world.

In a recent case, Buhtrap operators were able to compromise a SWIFT administrator workstation, granting them the power to issue fraudulent SWIFT requests. The initial compromise was through a spear-phishing email sent directly to the SWIFT administrator with a *Word* document in an attachment. This document, supposedly detailing a conference for bank employees, was in fact built with Microsoft Word Intruder and thus contained code to exploit several known *Word* vulnerabilities. A couple of weeks elapsed before the heist was conducted. The fraudsters could use this time to gain knowledge of the bank's employee behaviour and how best the heist could be performed. Soon thereafter, the bank registered a loss of close to 100 million rubles and lost its licence in the aftermath. While we do not know with certainty who was behind the fraud, we know that the bank was targeted by the Buhtrap gang.

Attacks on trading terminals

Having access to a trading terminal can bring significant benefits to the cybercriminals. The case we will discuss here is an attack on the Russian ruble exchange rate that allowed traders to make money on the strong variation that resulted. While direct usage of the terminal to influence stock or currency price is an option, cybercriminals can also gain insider information that they can leverage to make gains on the stock market.

The February 2015 attack on a trading terminal by the Corkow group was not a surprise for those who have tracked the associated malware family since its inception. The Corkow group focused on trading platforms almost from the beginning. It has specialized plug-ins, called DC, which can be used to extract information from these systems. Once executed, it collects browsing history, installed software, and running processes. It looks specifically for online banking applications, whether the user has visited sites for traders lately, or has installed applications for trading such as *Finam Direct II*, *BlackWood Pro*, *Scottrade*, *QuoteTracker*, *eSignal*, *TraderBytes*, *ROX*, *Interactive Brokers*, and others. In the third quarter of 2014, two new Corkow plug-ins made their appearance: QUIK and TRZQ. These modules are aimed at collecting credentials, account balance, settings, and other valuable information from two trading systems: *QUIK Workstation* and *TRANSAQ*.

One major incident, investigated by *Group-IB*, happened in a Russian bank located in Kazan [19]. According to their analysis, one of this bank's computers was successfully infected with Corkow.

This computer was used by bank employees as a trading terminal on the Moscow Exchange. While the attack occurred on 27 February 2015, the computer was infected by Corkow in September 2014. During this timeframe, malware operators were gathering information about the system and preparing for the attack. On Friday 27 February, when the bank employee was having lunch, malware operators placed a set of orders to buy and sell US$ on behalf of the bank. These orders resulted in the bank buying US$159 million and selling over US$94 million. These orders greatly affected the RUB/US$ rate, which swung between 55 and 66 RUB/US$ – a range an order of magnitude larger than normal. Fourteen minutes after the first order was passed, malware operators stopped issuing orders and wiped the trading terminal's disk drive in an attempt to hide traces of the attack.

The bank lost US$3.2 million during that period. However, it is still unclear whether the attackers gained any profit from this incident as vast sums of money were needed to make any significant profit.

Attacks on АРМ КБР (AWS CBC)

Russian banks use a special system to transfer funds between themselves. A bank combines all payments made during a given period of time to other Russian banks in a settlement batch (банковский рейс). When the batch is ready to be sent, the bank signs and encrypts the data using special software called *Automated Working Station of the Central Bank Client* (*AWS CBC*) and sends it to the Central Bank of Russia. A bank will usually send such a batch five times per day. The *AWS CBC* software is freely available on the Central Bank official website.

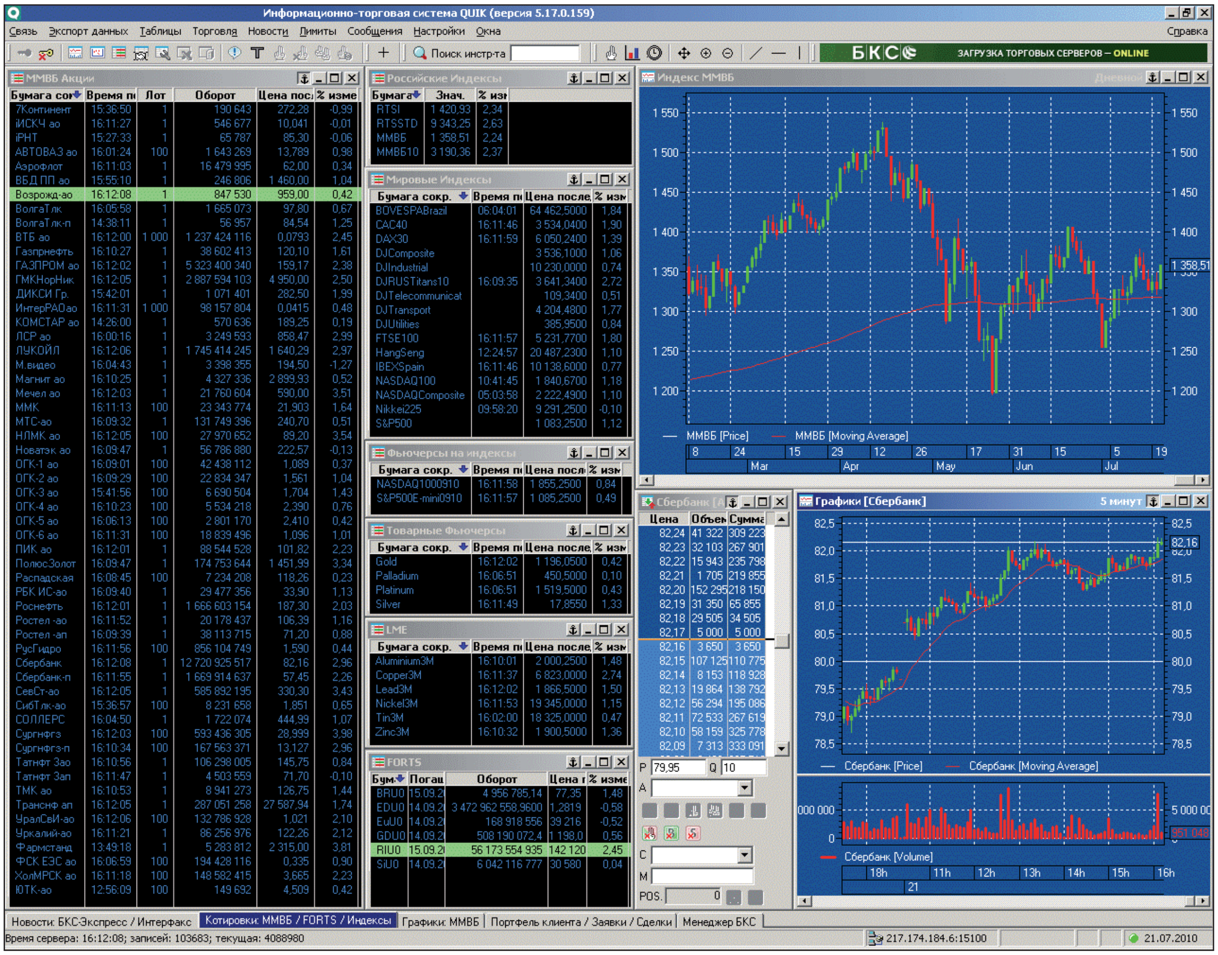
When attackers successfully compromise a machine with this software installed, they can alter data in the settlement batch before such data can be signed and encrypted. For example, attackers can modify the destination account so that the transfer will be made to bank accounts controlled by attackers instead of their original destination. Alternatively, the attackers can just add new entries to the settlement batch. This is possible because the *AWS CBC* software does not verify the integrity or validity of the data. It is the responsibility of the banks to ensure that this data cannot be accessed and modified by unauthorized users.

Both Buhtrap and Corkow actively search for computers with this software running by looking for uarm.exe in the active process list. Once they find a candidate, they can install remote administration software to log into the computer remotely and try to update the aforementioned records.

FUTURE ATTACKS

We have surveyed several attacks that occurred against Russian financial institutions in this paper. How likely are we to see the same techniques applied to other regions of the world?

First, we need to look at the reasons why these highly specialized groups are now targeting financial institutions. They are looking for financial gains, but also to maximize their return on investment. Looking at how these institutions were breached, via exploitation of old vulnerabilities, social engineering and



ММВБ Акции

Бумага сок	Время п	Лот	Оборот	Цена пос.	% изме
7Континент	15:36:50	1	190 643	272,28	-0,99
iИСКЧ ао	16:11:27	1	546 677	10,041	-0,01
iРНТ	15:27:33	1	65 787	85,30	-0,06
АВТОВАЗ ао	16:01:24	100	1 643 269	13,789	0,98
Аэрофлот	16:11:03	1	16 479 995	62,00	0,34
ВБД ПП ао	15:55:10	1	246 806	1 460,00	1,04
Возрожд-ао	16:12:08	1	847 530	959,00	0,42
ВолгаТлк	16:05:58	1	1 665 073	97,80	0,67
ВолгаТлк-п	14:38:11	1	56 957	84,54	1,25
ВТБ ао	16:12:00	1 000	1 237 424 116	0,0793	2,45
Газпрнефть	16:10:27	1	38 602 413	120,10	1,61
ГАЗПРОМ ао	16:12:02	1	5 323 400 340	159,17	2,38
ГМКНорНик	16:12:05	1	2 887 594 103	4 950,00	2,50
ДИКСИ Гр.	15:42:01	1	1 071 401	282,50	1,99
ИнтерРАОао	16:11:31	1 000	98 157 804	0,0415	0,48
КОМСТАР ао	14:26:00	1	570 636	189,25	0,19
ЛСР ао	16:00:16	1	3 249 593	858,47	2,99
ЛУКОЙЛ	16:12:06	1	1 745 414 245	1 640,29	2,97
М.видео	16:04:43	1	3 398 355	194,50	-1,27
Магнит ао	16:10:25	1	4 327 336	2 899,93	0,52
Мечел ао	16:12:03	1	21 760 604	590,00	3,51
ММК	16:11:13	100	23 343 774	21,903	1,64
МТС-ао	16:09:32	1	131 749 396	240,70	0,51
НЛМК ао	16:12:05	100	27 970 652	89,20	3,54
Новатэк ао	16:09:47	1	56 786 880	222,57	-0,13
ОГК-1 ао	16:09:01	100	42 438 112	1,089	0,37
ОГК-2 ао	16:09:29	100	22 834 347	1,561	1,04
ОГК-3 ао	15:41:56	100	6 690 504	1,704	1,43
ОГК-4 ао	16:10:23	100	5 534 218	2,390	0,76
ОГК-5 ао	16:06:13	100	2 801 170	2,410	0,42
ОГК-6 ао	16:11:31	100	18 839 496	1,096	1,01
ПИК ао	16:12:01	1	88 544 528	101,82	2,23
ПолюсЗолот	16:09:47	1	174 753 644	1 451,99	3,34
Распадская	16:08:45	100	7 234 208	118,26	0,23
РБК ИС-ао	16:09:40	1	29 477 356	33,90	1,13
Роснефть	16:12:01	1	1 666 603 154	187,30	2,03
Ростел -ао	16:11:52	1	20 178 437	106,39	1,16
Ростел -ап	16:09:39	1	38 113 715	71,20	0,88
РусГидро	16:11:56	100	856 104 749	1,590	0,44
Сбербанк	16:12:08	1	12 720 925 517	82,16	2,96
Сбербанк-п	16:11:55	1	1 669 914 637	57,45	2,26
СевСт-ао	16:12:05	1	585 892 195	330,30	3,43
СибТлк-ао	15:36:57	100	8 231 658	1,851	0,65
СОЛЛЕРС	16:04:50	1	1 722 074	444,99	1,07
Сургнфгз	16:12:03	100	593 436 305	28,999	3,98
Сургнфгз-п	16:10:34	100	167 563 371	13,127	2,96
Татнфт 3ао	16:10:56	1	106 298 005	145,75	0,84
Татнфт 3ап	16:11:47	1	4 503 559	71,70	-0,10
ТМК ао	16:10:53	1	8 941 273	126,75	1,44
Транснф ап	16:12:05	1	287 051 258	27 587,94	1,74
УралСвИ-ао	16:12:06	100	132 786 928	1,021	2,10
Уркалий-ао	16:11:21	1	86 256 976	122,26	2,12
Фармстанд	13:49:18	1	5 283 812	2 315,00	3,81
ФСК ЕЭС ао	16:06:59	100	194 428 116	0,335	0,90
ХолМРСК ао	16:11:18	100	148 582 415	3,665	2,23
ЮТК-ао	12:56:09	100	149 692	4,509	0,42

Российские Индексы

Бумага	Знач.	% изм
RTSI	1 420,93	2,34
RTSSTD	9 343,25	2,63
ММВБ	1 358,51	2,24
ММВБ10	3 190,36	2,37

Мировые Индексы

Бумага сокр.	Время п	Цена после	% изм
BOVESPABrazil	06:04:01	64 462,5000	1,84
CAC40	16:11:46	3 534,0400	1,90
DAX30	16:11:59	6 050,2400	1,39
DJComposite		3 536,1000	1,06
DJIndustrial		10 230,0000	0,74
DJRUSTitans10	16:09:35	3 641,3400	2,72
DJTelecommunicat		109,3400	0,51
DJTransport		4 204,4800	1,77
DJUtilities		385,9500	0,84
FTSE100	16:11:57	5 231,7700	1,80
HangSeng	12:24:57	20 487,2300	1,10
IBEXSpain	16:11:46	10 138,6000	0,77
NASDAQ100	10:41:45	1 840,6700	1,18
NASDAQComposite	05:03:58	2 222,4900	1,10
Nikkei225	09:58:20	9 291,2500	-0,10
S&P500		1 083,2500	1,12

Фьючерсы на индексы

Бумага сокр.	Время п	Цена посл	% изм
NASDAQ1000910	16:11:58	1 855,2500	0,84
S&P500E-mini0910	16:11:57	1 085,2500	0,49

Товарные Фьючерсы

Бумага сокр.	Время п	Цена после	% изм
Gold	16:12:02	1 196,0500	0,42
Palladium	16:06:51	450,5000	0,10
Platinum	16:06:51	1 519,5000	0,43
Silver	16:11:49	17,8550	1,33

LME

Бумага сокр.	Время п	Цена после	% изм
Aluminium3M	16:10:01	2 000,2500	1,48
Copper3M	16:11:37	6 823,0000	2,74
Lead3M	16:12:02	1 866,5000	1,50
Nickel3M	16:11:53	19 345,0000	1,15
Tin3M	16:02:00	18 325,0000	0,47
Zinc3M	16:10:32	1 900,5000	1,36

FORTS

Бум.	Погаш	Оборот	Цена	% изме
BRU0	15.09.2	4 956 785,14	77,35	1,48
EDU0	14.09.2	3 472 962 558,9600	1,2819	-0,58
EuU0	14.09.2	168 918 556	39 216	-0,52
GDU0	14.09.2	508 190 072,4	1 198,0	0,56
RIU0	15.09.2	56 173 554 935	142 120	2,45
SiU0	14.09.2	6 042 116 777	30 580	0,04

Сбербанк [А

Цена	Объем	Сумма
82,24	41 322	309 223
82,23	32 103	267 901
82,22	15 943	235 798
82,21	1 705	219 855
82,20	152 295	218 150
82,19	31 350	65 855
82,18	29 505	34 505
82,17	5 000	5 000
82,16	3 650	3 650
82,15	107 125	110 775
82,14	8 153	118 928
82,13	19 864	138 792
82,12	56 294	195 086
82,11	72 533	267 619
82,10	58 159	325 778
82,09	7 313	333 091

P 79,95 Q 10

A

C

M

POS. 0

Новости: БКС-Экспресс / Интерфакс | Котировки: ММВБ / FORTS / Индексы | Графики: ММВБ | Портфель клиента / Заявки / Сделки | Менеджер БКС

Время сервера: 16:12:08; записей: 103683; текущая: 4088980

217.174.184.6:15100

21.07.2010

Figure 7: QUIK application.

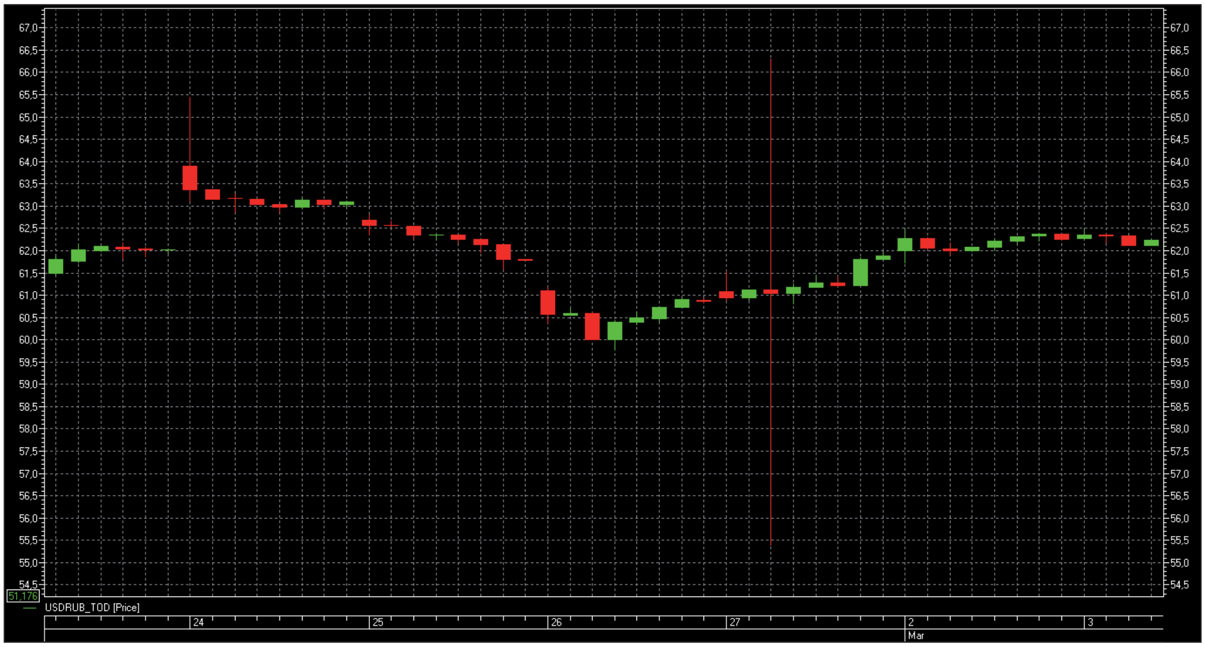


Figure 8: Anomaly caused by Corkow group in RUB/US$ exchange rate on 27 February 2015.

usage of third-party tools, it is not a surprise that seasoned cybercriminals are targeting them. While some institutions have good patching practices and other strong computer security procedures, a lot of them still don't. They represent the low-hanging fruit for these criminal groups, who are now experts in financial fraud. It is thus very likely that we will see similar attacks against financial institutions in other countries in the near future.

In fact, this has already started, with several cases being publicized concerning cybercriminals able to compromise workstations used by SWIFT administrators and using those to wire huge sums of money to foreign accounts. The heist against Bangladesh Bank, the central bank of Bangladesh, where fraudsters attempted to wire US$951 million, is a prime example. While most of the transfers were blocked, several millions are still unaccounted for.

The other question is whether all of the techniques we have looked at might be used against other banks or banks in the western world. We will see how this will unfold, but as some targeted Russian banks had strong security measures in place, we can expect these types of attack to succeed at some point against banks in all regions of the world.

CONCLUSION

We have reviewed different attacks against financial institutions in Russia and ascertained that these types of attacks and the techniques used are already spreading to the rest of the world. While the groups perpetrating these attacks are highly specialized and efficient, they are benefiting from the general lack of awareness surrounding targeted attacks against the financial sector. The attacks described in this paper are generally made possible initially through old vulnerabilities or social engineering. Regular patching of software, employee training and wide usage of two-factor authentication should help mitigate these attacks. There are more and more similarities between APT groups and cybercriminals targeting financial institutions. Besides the techniques used, another similarity is the way in which both groups achieve success by targeting the weakest link in the chain: the human factor.

REFERENCES

[1] FinCERT goals. «ФинЦЕРТ» Банка России. http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=fincert, webpage retrieved in June 2016.

[2] Interfax Russia. ЦБ заподозрил банки в использовании кибератак для вывода средств. http://www.interfax.ru/business/494833, webpage retrieved in June 2016.

[3] Cherepanov, A.; Lipovksy, R. Corkow: Analysis of a business-oriented banking Trojan. 2014. http://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/.

[4] Rudnitsky, J.; Khrennikov, I. Russian Hackers Moved Ruble Rate With Malware. Bloomberg. 2016. http://www.bloomberg.com/news/articles/2016-02-08/russian-hackers-moved-currency-rate-with-malware-group-ib-says.

[5] Shestopal, O. Мошенники нанесли удар по ОРС. Kommersant.ru. 2016.http://www.kommersant.ru/doc/2795587.

[6] Group-IB; Fox-IT. Anunak: APT Against Financial Institutions. December 2014. http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf.

[7] Kaspersky Lab. Carbanak APT, The Great Bank Robbery. February 2015. https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

[8] Sanger, E. D.; Perlroth, N. Bank Hackers Steal Millions via Malware. The New York Times. February 2015. http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0.

[9] Boutin, J.-I. Operation Buhtrap, the Trap for Russian Accountants. April 2015. http://www.welivesecurity.com/2015/04/09/operation-buhtrap/.

[10] Group-IB. Buhtrap, the Evolution of Targeted Attacks against Financial Institutions. March 2016. http://www.group-ib.com/brochures/gib-buhtrap-report.pdf.

[11] Stoyanov, R. Russian Financial Cybercrime: How It Works. Securelist. November 2015. https://securelist.com/analysis/publications/72782/russian-financial-cybercrime-how-it-works/.

[12] Kafeine. Meet Niteris EK (formerly known as CottonCastle). April 2014. http://malware.dontneedcoffee.com/2014/06/cottoncastle.html.

[13] Villeneuve, N; Homan, J. A New Word Document Exploit Kit. April 2015. https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html.

[14] Matrosov, A. All Carberp botnet organizers arrested. July 2012. http://www.welivesecurity.com/2012/07/02/all-carberp-botnet-organizers-arrested/.

[15] Szappanos, G. Microsoft Word Intruder Revealed. August 2015. https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf.

[16] Symantec. February 2016. http://www.symantec.com/connect/blogs/russian-bank-employees-received-fake-job-offers-targeted-email-attack.

[17] Boutin, J-I. Operation Buhtrap malware distributed via ammyy.com. November 2015. http://www.welivesecurity.com/2015/11/11/operation-buhtrap-malware-distributed-via-ammyy-com/.

[18] Kaspersky. Carbanak and beyond: banks face new attacks. February 2016. http://www.kaspersky.com/about-us/news/virus/2016/Carbanak-and-beyond-banks-face-new-attacks.

[19] Group-IB. Analysis of Attacks Against Trading and Bank Card Systems. 2016. http://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf.